Australian Government
Australian Institute of Criminology

Understanding online fraud victimisation in Australia

15th International Symposium of World Society of Victimology

Dr. Monique Mann, Mr. Anthony Morgan and Dr. Marcus Smith
Australian Institute of Criminology

Online Fraud

- Four defining elements of online fraud (Cross, Smith & Richards, 2014)

1. Via the internet
2. Dishonest invitation, request, notification or offer
3. Provide personal information or money
4. Financial or non-financial loss or impact of some kind

$1.4 billion lost to personal fraud

1.2 million Australian victims

Source	Jurisdiction	Sample size	Key findings
Reyns (2013)	United Kingdom	5,985	Internet banking, IM, emailing, males, older persons, higher incomes, perceive risk have increased likelihood of being a victim of identity theft.
Leukfeldt (2014)	Europe (Netherlands)	10,316	Demographic and financial characteristics did not impact the likelihood of phishing victimisation. Antivirus software had no impact on victimisation.
Reisig, Pratt & Holtfreter (2009)	United States (Florida)	573	Demographics (socially vulnerable, lower socio-economic status) influence risk perception. Individuals with higher perceived risk spend less time online and make fewer online purchases

Source	Jurisdiction	Sample size	Key findings
Reyns (2013)	United Kingdom	5,985	Internet banking, IM, emailing, males, older persons, higher incomes, perceive risk have increased likelihood of being a victim of identity theft.
Leukfeldt (2014)	Europe (Netherlands)	10,316	Demographic and financial characteristics did not impact the likelihood of phishing victimisation. Antivirus software had no impact on victimisation.
Reisig, Pratt & Holtfreter (2009)	United States (Florida)	573	Demographics (socially vulnerable, lower socio-economic status) influence risk perception. Individuals with higher perceived risk spend less time online and make fewer online purchases

Source	Jurisdiction	Sample size	Key findings
Reyns (2013)	United Kingdom	5,985	Internet banking, IM, emailing, males, older persons, higher incomes, perceive risk have increased likelihood of being a victim of identity theft.
Leukfeldt (2014)	Europe (Netherlands)	10,316	Demographic and financial characteristics did not impact the likelihood of phishing victimisation. Antivirus software had no impact on victimisation.
Reisig, Pratt & Holtfreter (2009)	United States (Florida)	573	Demographics (socially vulnerable, lower socio-economic status) influence risk perception. Individuals with higher perceived risk spend less time online and make fewer online purchases

Source	Jurisdiction	Sample size	Key findings
Reyns (2013)	United Kingdom	5,985	Internet banking, IM, emailing, males, older persons, higher incomes, perceive risk have increased likelihood of being a victim of identity theft.
Leukfeldt (2014)	Europe (Netherlands)	10,316	Demographic and financial characteristics did not impact the likelihood of phishing victimisation. Antivirus software had no impact on victimisation.
Reisig, Pratt & Holtfreter (2009)	United States (Florida)	573	Demographics (socially vulnerable, lower socio-economic status) influence risk perception. Individuals with higher perceived risk spend less time online and make fewer online purchases

Routine Activity Theory (Cohen & Felson, 1979)

Suitable target

Absence of a capable guardian

Motivated offender

What is the relationship between victimisation and:

- Perceived risk
- Prevention behaviour
- Demographics
- Online activities

Method and Analytic Approach

Online fraud victimisation (n=1,786)

	n	%
Victim	345	19.32
Not Victim	1,441	80.68

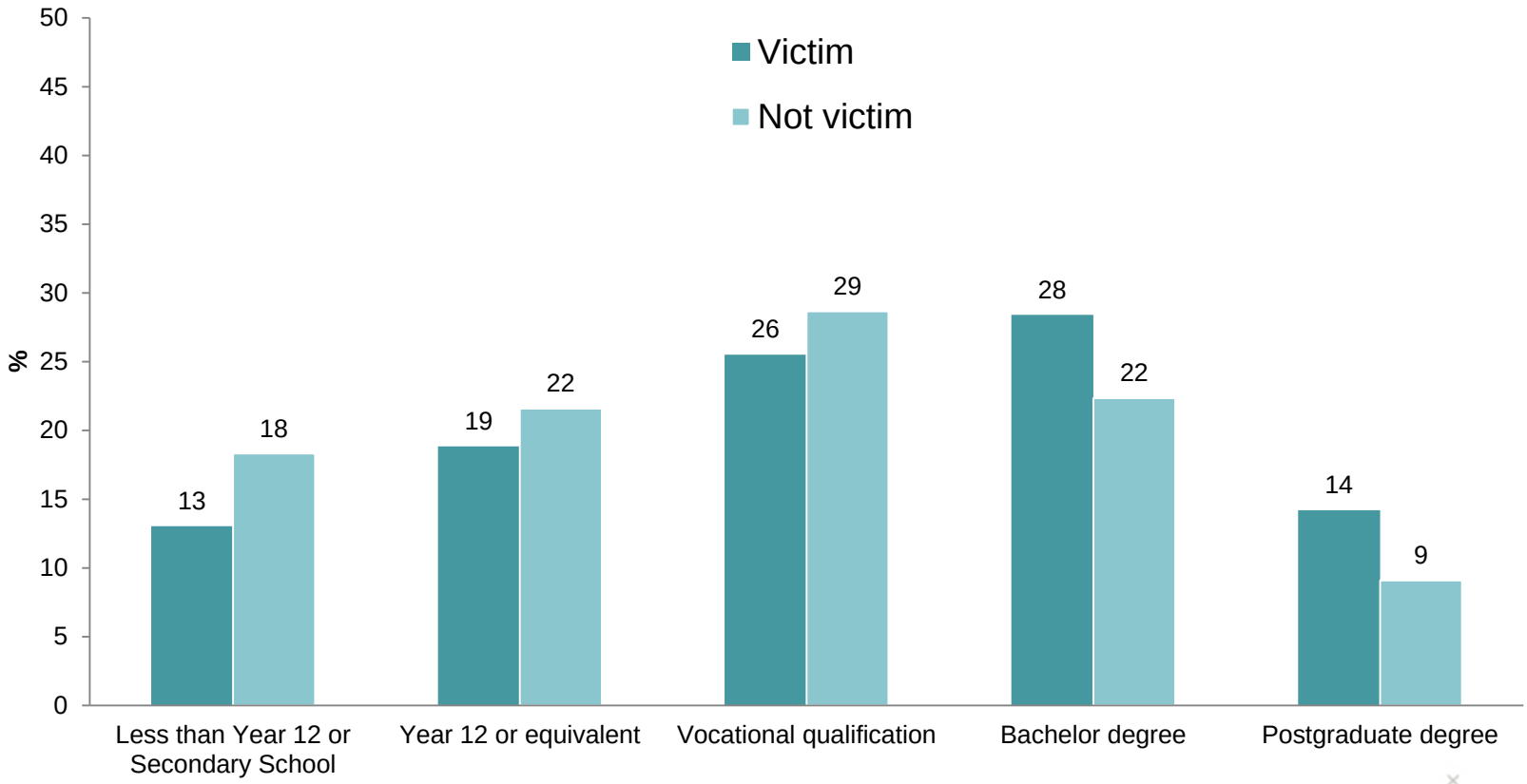
Category	Independent Variables
Demographics	Gender
	Age
	Education
	Income
Online activities	Social media use
	Tablet use
	Online shopping
Preventative behaviour	Passwords
	Security measures including anti-virus
	Financial protection
	Spam filters
	Interact with known persons only

Category	Independent Variables
Demographics	Gender
	Age
	Education
	Income
Online activities	Social media use
	Tablet use
	Online shopping
Preventative behaviour	Passwords
	Security measures including anti-virus
	Financial protection
	Spam filters
	Interact with known persons only

Category	Independent Variables
Demographics	Gender
	Age
	Education
	Income
Online activities	Social media use
	Tablet use
	Online shopping
Preventative behaviour	Passwords
	Security measures including anti-virus
	Financial protection
	Spam filters
	Interact with known persons only

Australian Government
Australian Institute of Criminology

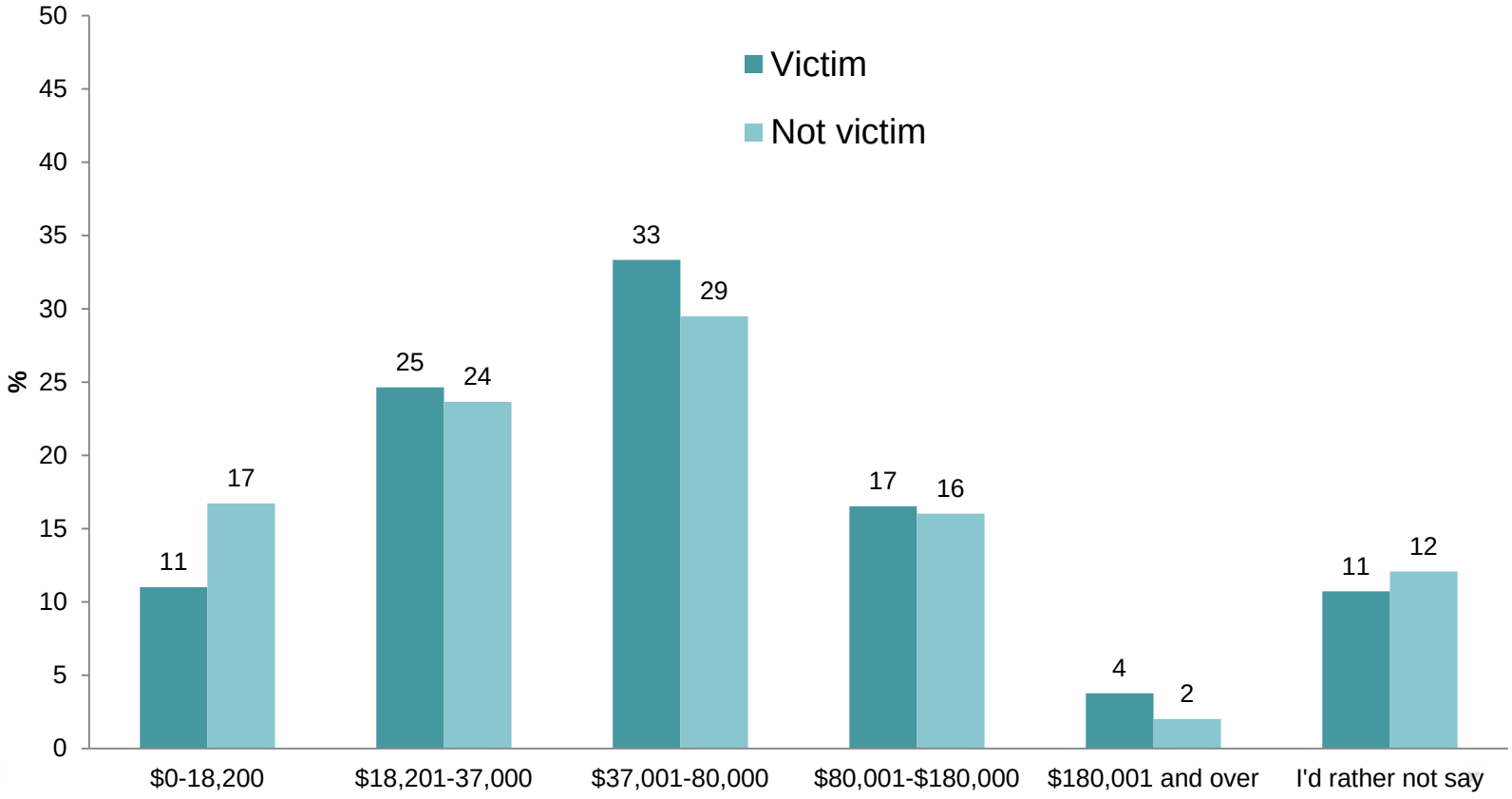
Relationship between education and victimisation



χ^2 (4, n= 1,786) = 18.03, p.<.001, Cramer's V= 0.1 (small effect size)

Australian Government
Australian Institute of Criminology

Relationship between income and victimisation

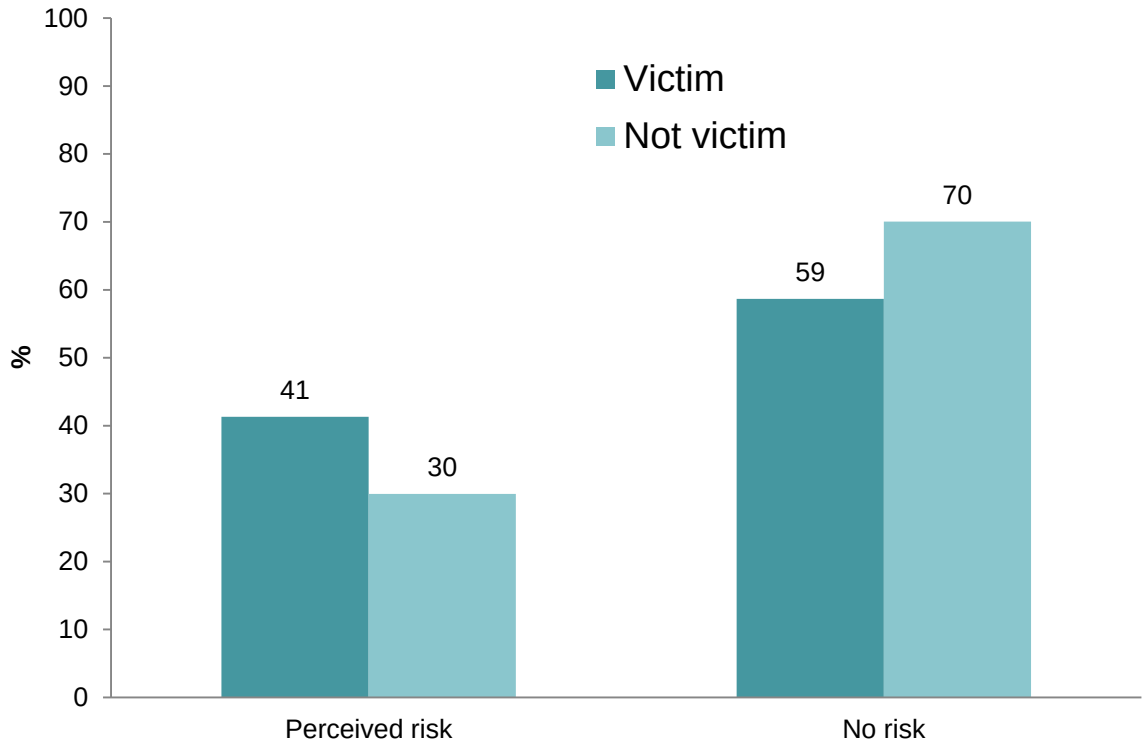


χ^2 (5, n= 1,786) = 11.40, p.<.05, Cramer's V= 0.08 (small effect size)

Relationship between online shopping and victimisation

χ^2 (5, n= 1,786) = 80.40, p.<.000, Cramer's V= 0.21 (medium effect size)

Relationship between risk perception and victimisation



χ^2 (1, n=1,703) = 15.90, p.<.000, Cramer's V= 0.1 (small effect size)

Logistic Regression Predicting Victimisation

Predictors	Odds Ratio (Ψ)	95%CIΨ	p<
Income			
$80,001-$180,000 (vs $37,001-$80,000)	0.68	0.47-1.00	.05
Online shopping			
Every 2-3 months (vs 2-3 times a month)	0.56	0.39-0.80	.01
Less often than 2-3 months (vs 2-3 times a month)	0.35	0.23-0.55	.001
Never (vs 2-3 times a month)	0.34	0.16-0.75	.01
Weekly or more often (vs 2-3 times a month)	1.86	1.26-2.74	.01
Risk perception (vs no risk perception)	1.40	1.07-1.81	.05

Model: $\chi 2$ (df=18, n= 1,703) = 102.34, p<.05, AUC = 0.67, Pseudo R2 = 0.06, Cox & Snell R2=0.06, Nagelkerke R2= 0.09

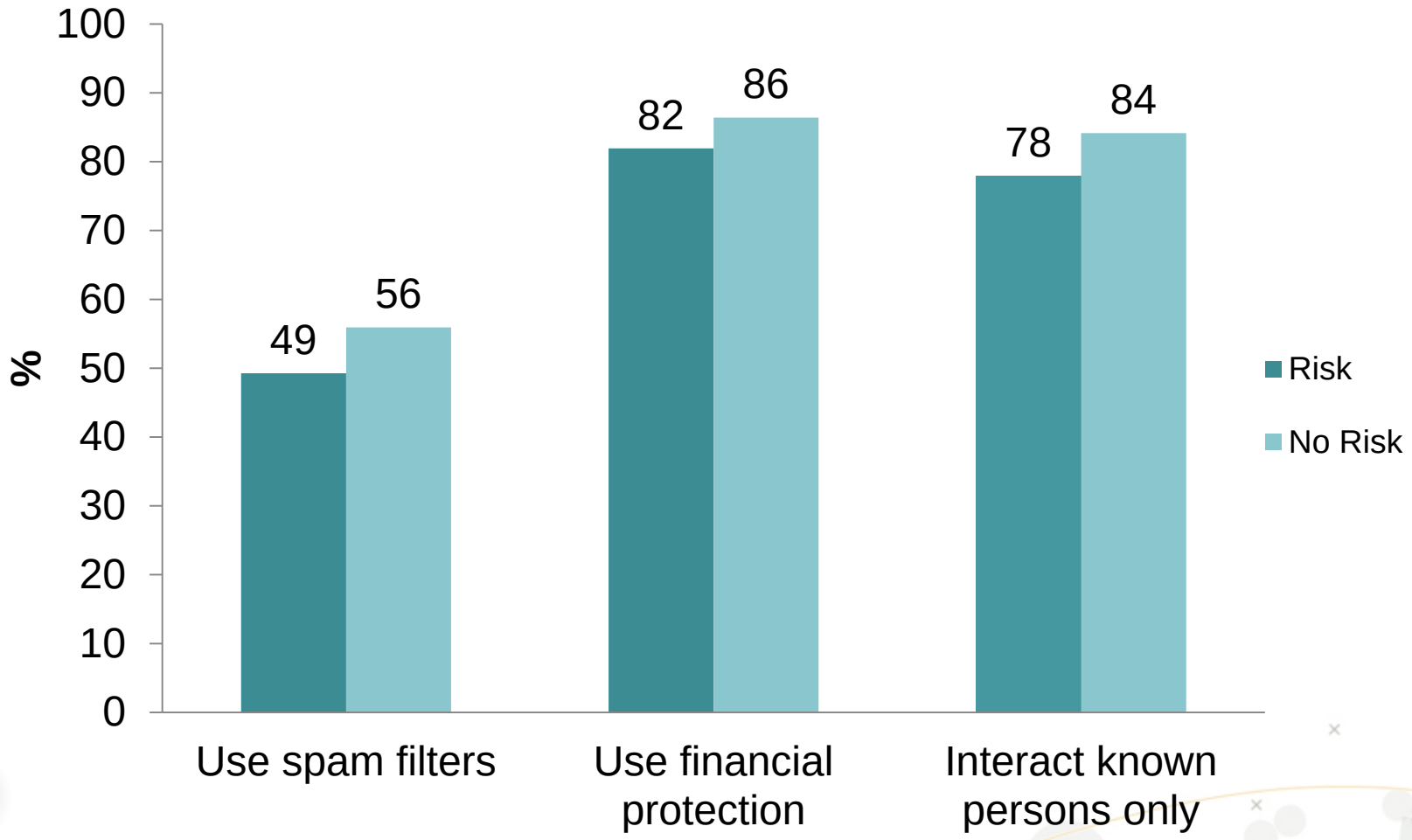
Risk factors:

1. **Income**
   - $37,001-$80,000
2. **Frequent online shoppers**
   - Weekly or more often
   - 2-3 times per month
   - Every 2-3 months
   - Less often than 2-3 months
   - Never
3. **Risk perception**

Key findings

- Complicated risk profile, divergences with traditional victim profile
- Analysis has gone a little further, but only explains a small amount of risk
- Need to take a more nuanced approach to understanding online fraud

Relationship between risk perception and prevention behaviour



The way forward

- Examine what influences the likelihood of victimisation for other online crimes (e.g. attacks on computer system and virus), and differences for sub-categories of online fraud (e.g. romance scams versus work from home scams)

- Investigate protective factors and impact of preventative strategies for specific sub-categories of online fraud

- Examine characteristics and predictors of online repeat victims, limited literature that examines repeat victimisation in online context

QUESTIONS?

Contact: Monique.Mann@aic.gov.au